(12) UK Patent Application (19) GB (11) 2 316 841 (13) A

(43) Date of A Publication 04.03.1998

(21) Application No 9718374.3

(22) Date of Filing 29.08.1997

(30) Priority Data
(31) 08227969 (32) 29.08.1996 (33) JP

(51) INT CL[6]
H04L 9/32

(52) UK CL (Edition P)
H4P PPEB
H4L LDSC

(58) Field of Search
UK CL (Edition O) H4P PPEB
INT CL[6] H04L 9/32 12/22 29/06
Online:- WPI, INSPEC, JAPIO

(71) Applicant(s)
Kokusai Denshin Denwa Co Ltd

(Incorporated in Japan)

3-2 Nishishinjuku 2-chome, Shinjuku-ku, Tokyo 163, Japan

(72) Inventor(s)
Ayumu Kubota
Kazuki Katagishi
Tohru Asami

(74) Agent and/or Address for Service
Boult Wade Tennant
27 Furnival Street, LONDON, EC4A 1PQ, United Kingdom

(56) Documents Cited
INSPEC Abstract No.B9502-6210L-059, C9502-5620W-012 & Tenth Comp. Sec. Conference,1994,IEEE,pp212-18

(54) Method for controlling a firewall

(57) When a mobile terminal 21 connected to an Internet service provider (ISP) 30 intends to access an inner network 20 within a firewall 22 via the Internet 10, the ISP sends terminal user information to the inner network. An agent host 32 investigates the Internet protocol (IP) address and the account of the terminal and determines whether the mobile terminal is a terminal moved from the inner network based on this information. If this is the case, a host 23 managing the firewall sets a filter in the firewall allowing telecommunication between the mobile terminal and the inner network. The communication between the terminal and inner network may be by means of a two-way IP tunnel 40.

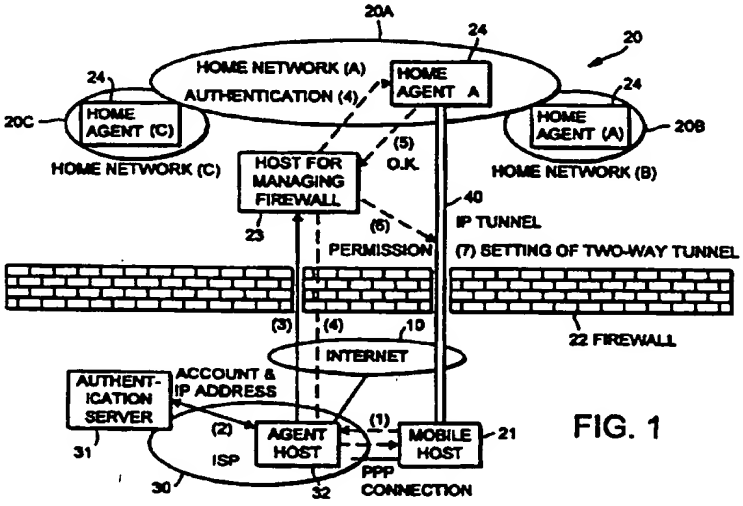

FIG. 1

At least one drawing originally filed was informal and the print reproduced here is taken from a later filed formal copy.

This print takes account of replacement documents submitted after the date of filing to enable the application to comply with the formal requirements of the Patents Rules 1995

GB 2 316 841 A

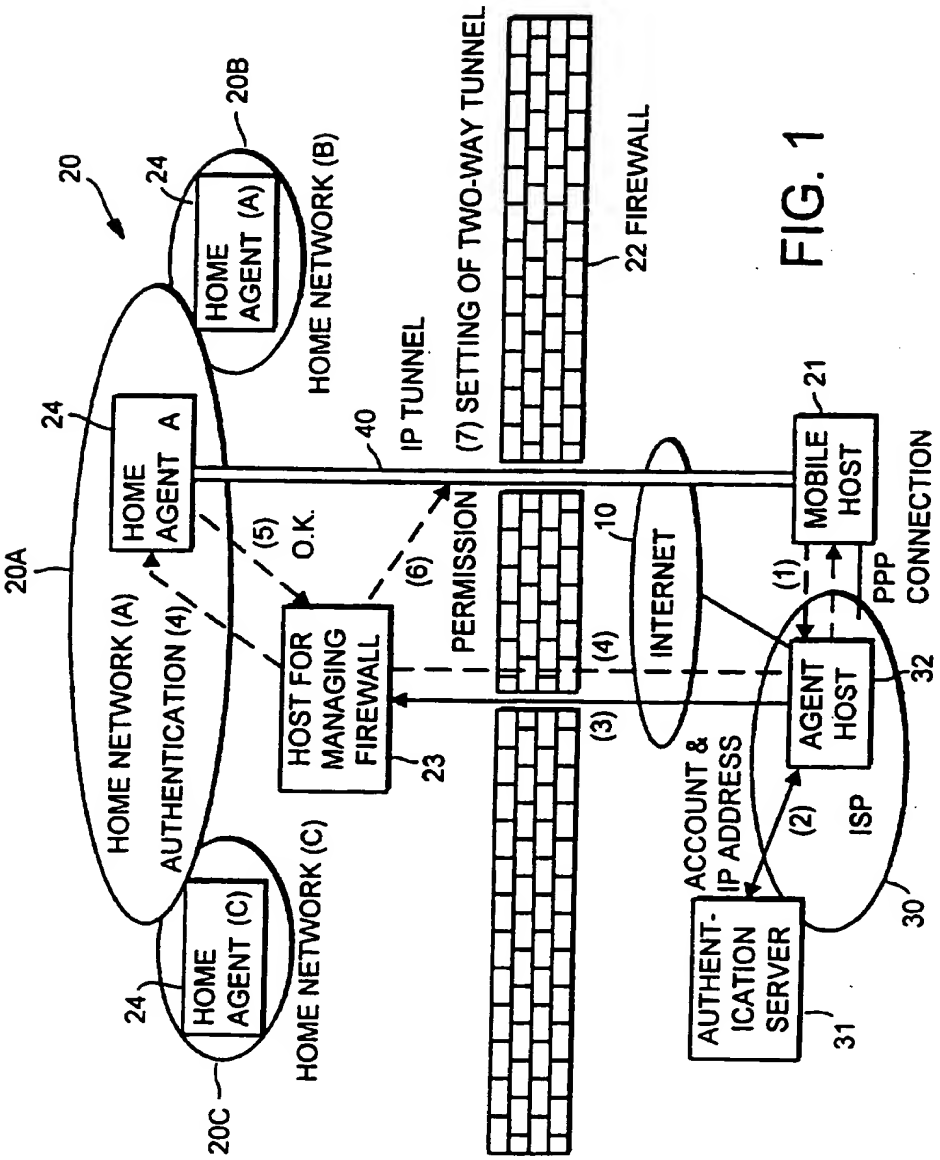
20
20A
20B
20C
24
HOME AGENT A
HOME AGENT (A)
HOME AGENT (C)
HOME NETWORK (A)
HOME NETWORK (B)
HOME NETWORK (C)
AUTHENTICATION (4)
(5) O.K.
(6) PERMISSION
40
IP TUNNEL
(7) SETTING OF TWO-WAY TUNNEL
22 FIREWALL
HOST FOR MANAGING FIREWALL
23
10
INTERNET
(1)
(2)
(3)
(4)
MOBILE HOST
21
PPP CONNECTION
AGENT HOST
32
ISP
30
ACCOUNT & IP ADDRESS
AUTHENT-ICATION SERVER
31

FIG. 1

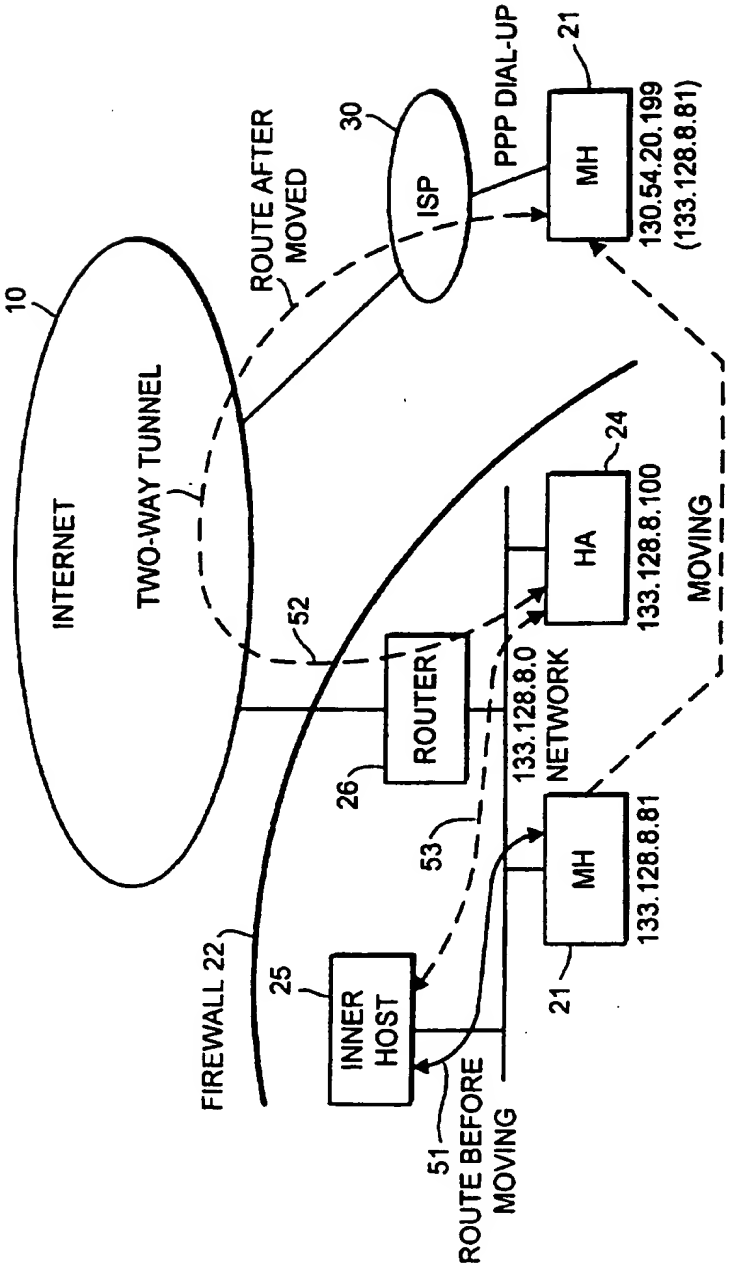

FIG. 2

MOBILE-IP (ADAPTIVE TO FIREWALL)

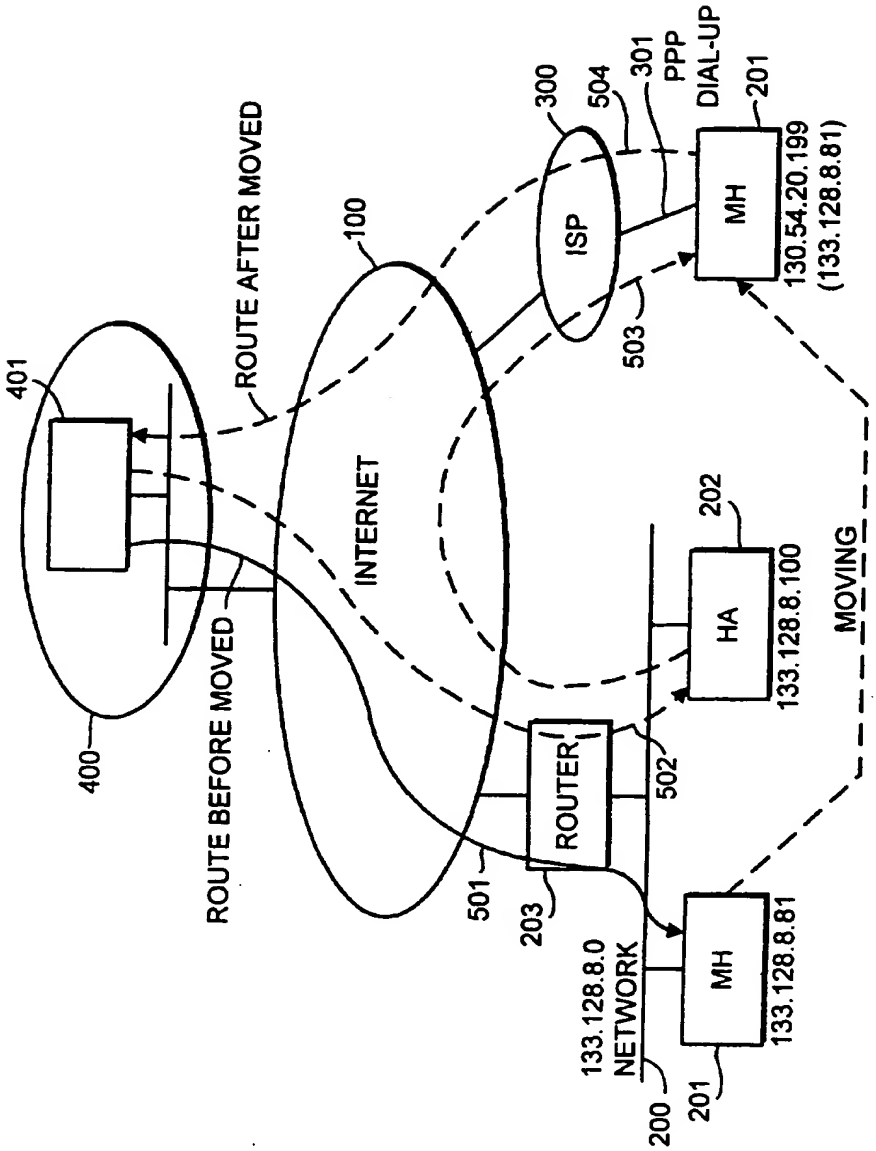

FIG. 3

PRIOR ART MOBILE-IP (NOT ADAPTIVE TO FIREWALL)

Specification

TITLE OF THE INVENTION

Method for dynamically controlling a firewall

FIELD OF THE INVENTION

This invention relates to a method for dynamically controlling a firewall.

BACKGROUND OF THE INVENTION

In a case of connecting a private network with the Internet, it is necessary to prevent a dishonest access from the Internet. However, if perfectly shut down a telecommunication between an internal network and an external network, it is impossible for a user of the internal network to access to his home network via the Internet.

Therefore, it is necessary to construct a firewall which selectively permits a telecommunication from an outside via the Internet.

In a prior art of a firewall, out of all data packets between the internal network and the external network, a previously permitted packet is only passed, but, another packet is shut down by using a filter.

Generally, such a filter is set by designating an IP (Internet Protokol) address of a terminal sending a packet, an IP address of a terminal receiving the packet, a kind of used protokol and a port number etc. For example, in a case of a telecommunication from an specific external IP address to any internal host (terminal) by using TCP (Transmission Control Protokol), a telecommunication using a specific port number (for example, 110) is permitted.

Wherein, the port number is an identifier for indicating a process of an upper layer in TCP or UDP (User Datagram Protokol).

However, it is difficult to obtain a pertinent filtering when a

user accesses to his home network, by a dial-up or ppp connection via an ISP (Internet Service Provider) at outside of the home network, by using a mobile computer such as a note-type personal computer (a note-type PC), because upper 4 digits indicates a network with which the mobile PC is connected and lower 4 digits indicates an identifier of the mobile PC in the network, while the IP address used in the Internet telecommunication is indicated by 4 bytes number.

Namely, in a case of dial-up connection by a mobile host (MH) moved from its home network, the IP address assigned to the mobile host is different every connection, then it is impossible to take a telecommunication using an IP address assigned in its home network.

THerefore, it is difficult to set a filter in the firewall by designating an IP (Internet Protokol) address of the terminal sending a data packet and an IP address of the terminal receiving the data packet, because an IP address of a moved terminal is not constant in the dail-up connection.

Furthermore, it is not always possible for the user to use inner resources (a disk, data base and WWW etc.) of the home network to which he usually accesses, even if the filter of the firewall is pertinently set and it is possible only for an authorized mobile host and its user to permit an access from outside to the home network, because an access to the inner resources is individually limited and the access is permitted or is not permitted based on an IP address of a client terminal.

Next, referring to Fig.3, a mobile-IP address is explained, the mobile-IP is under work for standardization.

The mobile IP is a technique which enables to use a same IP address to the mobile terminal which moves anywhere, whenever the mobile terminal connects the Internet.

However, now, the mobile-IP is not adaptive to a network having the firewall.

In Fig.3, 100 denotes the Internet, 200 denotes a home network of a mobile terminal 201, 202 denotes a home agent (HA) on the home network 200, 203 denotes a router, 300 denotes an ISP, 400 denotes another network and 401 denotes a terminal on the network 400.

In Fig.3, an IP address of the home network 200 to which the mobile terminal 201 is usually connected is [133.128.8.0], an IP address of the mobile terminal 201 on the home network 200 is [133.128.8.81], an IP address of the home agent 202 is [133.128.8.100], and, an IP address of the mobile terminal 201 is [130.54.20.199] which is assigned by the ISP when the terminal 201 connects to the ISP by dial-up connection.

Generally, when a packet is sent from the terminal 401 on the network 400 to the terminal 201, as a rout 501 shown in Fig.3, the packet is transferred to the home network 200 to which the terminal 201 is usually connected. Therefore, when the terminal has been moved to another network, for example the ISP 300, it is necessary to transfer the packet to the network 300.

For transferring the packet, in the mobile-IP, an agent host is respectively provided to the network from which the mobile terminal is moved and the network to which the mobile terminal is moved. The agent in the network from which the mobile terminal is moved is called as a home agent and the agent in the network to which the mobile terminal is moved is called as a foreign agent. It is possible that the mobile terminal has a function of the foreign agent. In Fig.3, the mobile terminal 201 has a function of the foreign agent.

When the terminal 201 moved from its home network 200 connects to the ISP 300 by dial-up connection 301, a temporary IP address [130.54.2

0.199] is assigned to the terminal 201 by the ISP.

The IP address [130.54.20.199] of the mobile terminal 201 and its IP address [133.128.8.81] in the home network 200 are informed to the home agent 202 in the home network 200 via the ISP and the Internet100. Then, the home agent 202 records that the terminal 201 having the IP [133. 128.8.81] is moving and its temporary IP address is [130.54.20.199] in its data base, based on the received information.

When a packet is sent from the terminal 401 in the network 400 to the terminal 201 by using the usual IP address [133.128.8.81], as shown by route 502, the home agent 202 receives the packet instead of the mobile terminal 201. Then, as shown by the route 503, the home agent 202 transfers the packet from the terminal 401 to the mobile terminal 201 via the Internet 100 and the ISP 300 to the mobile terminal 201, by embedding the packet from the terminal 401 into a packet forwarded to the temporary IP address [130.54.20.199]. The mobile terminal 201 obtains the original packet of the terminal 401 from the received packet, if necessary, as shown by the route 504, any packet to the terminal 401 via the ISP and the Internet.

As mentioned-above, in the mobile-IP, it is possible to a packet from the terminal 401 to the mobile terminal 201 by using the usual IP address [133.128.8.81].

However, the telecommunication using the temporary IP address [130. 54.20.199] is necessary between the mobile terminal 201 and the home agent 202.

Namely, in the mobile-IP, since any process is not applied to the packet send from the mobile terminal 201, an usual routing is necessary. Therefore, it is impossible for the mobile terminal 201 to another terminal inside the home network 200 except for the home agent 202 under the above-mentioned firewall, because only the telecommunication

between the mobile terminal 201 and the home agent 202 is allowed. This means that the mobile terminal 201 is limited to access to the resource of its home network 200.

An object of the present invention is to provide a method for dynamically controlling a firewall which enables to set a filter pertinent to the mobile terminal being connected with the ISP (Internet Service Provider) by the dial-up connection and its user.

An object of embodiments of the present invention is to provide a method for dynamically controlling a firewall which enables to pertinently permit that said mobile terminal and its user access to the resource of the home network from outside.

The present invention enables to set a pertinent filter by obtaining a user information from an Internet service provider. Embodiments of the present invention resolve an limitation of an access to a resource of a home network by combining the filter setting with a mobile-IP.

According to the present invention there is provided a method for enabling a pertinent filter comprising the steps of:

a step for sending a user information of a terminal being connected to an internet service provider by dial-up connection to an inner network inside a firewall from said internet service provider when said terminal accesses to said inner network via the Internet.

a step that said inner network determines whether said terminal is a mobile terminal moved from said inner network, based on said user information;

a step for setting a filter of said firewall to permit a telecommunication between said terminal when said terminal is said mobile terminal moved from said inner network.

In a method embodying the present invention, for resolving an limitation of an access, further an

IP tunnel is used after setting of said filter for a telecommunication between said terminal and inner network.

In another embodiment for resolving an limitation of an access, said user information is transferred between an agent host provided in said internet service provider and a host for managing said firewall which sets said filter of said firewall provided in said inner network, and said telecommunication using said IP tunnel is done between said terminal and a home agent provided in said inner network.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 shows a configuration of a system to which a method embodying the present invention is applied.

Fig. 2 shows a mobile-IP which is adaptive to a firewall.

Fig. 3 shows an prior art mobile-IP which is not adaptive to a firewall.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

An embodiment of the present invention will be explained referring to the drawings.

In Fig. 1, 10 denotes the Internet, 20 denotes an inner network having plural home networks 20A, 20B and 20C, 21 denotes a mobile terminal which is usually connected to the inner network 20, 22 denotes a firewall, 23 denotes a host for managing the firewall, 24 denotes a home agent provided in each of home networks 20A, 20B and 20C, 30 denotes an ISP (Internet Service Provider), 31 denotes a server for authentication in the ISP, 32 denotes an agent host in the ISP.

The mobile terminal 21 has a function of a foreign agent for mobile-IP. The mobile terminal 21 is intended to connect the inner network 20 via the Internet, by dial-up connection to the ISP at any location after moving from the home network.

In this embodiment, a mechanism for controlling the firewall based

on a user information obtained from the ISP and a mobile-IP mechanism adaptive to the firewall are provided.

The mechanism for controlling the firewall 22 based on the user information obtained from ISP 30 will be explained referring to Fig.1.

A user account (ID) and a pass word are input to the ISP 30, when a user of the mobile terminal 21 intends to connect to the ISP 30 by the dial-up connection. In the ISP 30, the authentication server 31 determines whether the user input data are proper or not. Only when the user input data are proper, an IP address is assigned to the mobile terminal 21, then the mobile terminal 21 is connected to the Internet 100. For this purpose, the ISP 30 can always grasp which user is connecting to the ISP 30 based on the user information and which IP address is assigned to the mobile terminal 21.

When the inner network 20 can know the user and an IP address used by the user, by obtaining the user information from the ISP 30, it is possible to properly set the filter. Then, it is possible to permit a telecommunication from a user who is previously allowed to access to the inner network 20 and to exclude an access from a user who has not authority for the access.

In Fig.1, a mechanism for adding and/or deleting a filter is provided, by providing the host 23 for managing the firewall within the inner network 20. Further, the agent host 32 is provided within the ISP so that only the telecommunication between the agent host 32 and the host 23 for managing the firewall can be allowed. Since the hosts 23 and 32 can use a fixed IP address for this telecommunication, there is no problem on setting the filter for the firewall.

Concretely, the filter is set by the following steps (1)~(7). The step (n) corresponds to an symbol (n) in Fig,1.

(1) When the mobile terminal 21 intends to access to the inner network

20 from outside of it, the mobile terminal 21 requests an establishment of the connection between the mobile terminal 21 and the inner network 20 via the the agent host 32 in the ISP.

(2) The agent host 32 investigates an IP address and an account at dial-up connection of the mobile terminal 21.

(3) The agent host 32 relays a message from the mobile terminal 21 to the host 23 for managing the firewall, only when the mobile terminal 21 is connected by using a specific account which is allowed to access inside the firewall 22.

(4) An authentication is done by end-to-end method between the mobile terminal 21 and the home agent 24 via the host 23 for managing the firewall, because, in mobile-IP, an authentication must be done between the mobile terminal and the home agent.

(5) If the authentication is successful, the home agent sends a message of the success to the host 23 for managing the firewall.

(6) Then, the host 23 for managing the firewall changes the setting of the firewall 22 so as to permit the telecommunication between the mobile terminal 21 and the home agent 24.

(7) At the time when the host 23 for managing the firewall enables the telecommunication between the mobile terminal 21 and the home agent 24 by changing the setting of the firewall 22, the host 23 informs it to the home agent 24 and the host 23 informs it to the mobile terminal 21 via the agent host 32. After receiving the message, the home agent 24 sets an IP tunnel to the mobile terminal 21 and the mobile terminal 21 sets an IP tunnel to the home agent 24, then a two-way IP tunnel 40 is set.

By using the two-way IP tunnel 40, the mobile terminal 21 telecommunicates with each terminal of the inner network 20. Wherein, the mobile terminal 21 periodically sends a message for maintaining the

connection to the host 23 for managing the firewall. When the message for maintaining the connection from a certain mobile terminal stops, the host 23 for managing the firewall automatically deletes the filter setting to the mobile terminal.

As mentioned above, it is possible to set the firewall 22 only within a necessary term and only for the telecommunication of which start point and end point are distinctly restricted.

A specification of the mobile-IP which is under work for standardization is not adaptive to the network 20 having the firewall 22.

Then, the mobile-IP is improved to adapt to the firewall 22 as follows, and the improved mobile-IP is combined with the above-mentioned filter setting.

An combination of the mobile-IP and the dynamic firewall control will be explained referring to Fig.2.

As a route 52 shown in Fig.2, a packet from the mobile terminal 21 to the terminal 25 inside the firewall 22 is embedded in a packet to the home agent 24, then sent out. The home agent 24 obtains an original packet out of the received packet. The home agent 24 sends the obtained packet to the inner terminal 25, as a route 53 shown in Fig.2, by sends again the obtained packet to the Internet. In Fig.2, 26 denotes a router. When the mobile terminal exist in the inner network 20, the mobile terminal 21 telecommunicates with the inner terminal 25 via a route 51.

As mentioned-above, even if an authority is individually allowed in the inner network 20, it is possible to permit the access based on the IP address of the mobile terminal 21 which is usually connected with the network 20 by using the two-way tunnel between the mobile terminal 21 and the home agent 24. Therefore, it is possible to

communicate between the mobile terminal 21 and the inner terminal 25.

According to the present invention, it is possible to set the firewall so as to permit the communication from the specific user in connection with the ISP by dail-up connection.

Further, according to embodiments of the present invention, because of an improvement and an combination of the mobile-IP, it is possible to access to the resources of the inner network from outside as same as connected with the inner network.

WHAT IS CLAIMED IS:

1. A method for dynamically controlling a firewall comprising steps of:

a step for sending a user information of a terminal being connected to an internet service provider by dial-up connection to an inner network inside a firewall from said internet service provider when said terminal accesses to said inner network via the Internet;

a step that said inner network determines whether said terminal is a mobile terminal moved from said inner network, based on said user information;

a step for setting a filter of said firewall to permit a telecommunication between said terminal when said terminal is said mobile terminal moved from said inner network.

2. The method claimed in claim 1 wherein, an IP tunnel is used after setting of said filter for a telecommunication between said terminal and said inner network.

3. The method claimed in claim 2 wherein, said user information is transferred between an agent host provided in said internet service provider and a host for managing said firewall which sets said filter of said firewall provided in said inner network, and said telecommunication using said IP tunnel is done between said terminal and a home agent provided in said inner network.

4. A method for dynamically controlling a firewall substantially as hereinbefore described with reference to the accompanying drawings.

The Patent Office

12

Application No: GB 9718374.3
Claims searched: 1-4

Examiner: Matthew Nelson
Date of search: 20 November 1997

Patents Act 1977
Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:

UK Cl (Ed.O): H4P (PPEB)

Int Cl (Ed.6): H04L 9/32, 12/22, 29/06

Other: Online:- WPI, JAPIO, INSPEC

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
X	INSPEC Abstract No. B9502-6210L-059, C9502-5620W-012 & "Tenth Annual Computer Security Applications Conference", published 1994, IEEE, pp212-18, Goldberg "The MITRE security perimeter" (see abstract).	

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.